

REMARKS

Applicant notes with appreciation the telephone interview afforded by the Examiner on August 27, 2002. The Examiner stated that she would rescind the finality of the office action in light of the following remarks.

Claim 13

Claim 13 stands rejected under 103 in light of Zampese. This rejection is respectfully traversed.

Claim 13 mentions three items: account number, account code, and signature phrase, which are further identified in the specification (pg. 7):

- (1) account number (A number that identifies an account. Example - a credit card number)
- (2) account code. (A number assigned to an account that indicates rights in the account, such as ownership. Example - a PIN. Note, a PIN does not identify an account, but is used to prove that you have rights to use the account.)
- (3) signature phrase. (A phrase associated with an account.)

It is clear from claim 13 that the signature phrase cannot be the same as the account number because that would make the claim indefinite. Also, while the present specification uses account *code* and signature phrase similarly for some embodiments, they are never equated to the account *number*.

Zampese discusses two types of numbers: an account code and a plurality of transaction codes. (4:44-45). The account code identifies an account. Zampese compares an account code with "a credit card number." (4:48). The transaction codes are intended to replace ordinary PINs or passwords. (4:49-52). In Zampese, an account management system gives each customer a list of transaction codes that are used for transactions (although the transaction codes must be used in the correct sequence). During a transaction, the customer gives his account code (credit card number) and the next transaction code on the list to the merchant, which then provides this information to the account management system. Since the account management system has a list of the transaction codes, it knows which is the next transaction code to be used and can thereby

validate the transaction. If a thief intercepts the transaction code during transmission, it will be of no value because each transaction code can only be used once.

Applicant believes that the primary confusion is the fact that the present application and Zampese use the term "account code" differently. Fortunately, both Zampese and the present application are very clear about what they mean when they refer to account codes. When comparing Zampese with the present application, the account *code* of Zampese should be compared with the account *number* of the present application. The transaction code of Zampese should then be compared with the account code/signature phrase of the present application. However, Zampese's transaction code is easily distinguished from the account code and signature phrase of the present application. In fact, Zampese himself distinguishes his transaction code from ordinary PINs and the like. (4:53-56).

Claim 22

Claim 22 stands rejected under 103 in light of Talati and Lineham. This rejection is respectfully traversed.

In claim 22, the term "authentication phrase" is a generic term that can include an account code or signature phrase. The authentication phrase from the user is being compared to another authentication phrase stored in the account entry in the authorization database. This is done at the authorization system (as specified in the claim element: "verifying that the received authentication phrase corresponds to an authentication phrase in the account entry.")

Talati, on the other hand, has the customer (also called user or originator, see 2:59-60) validate a unique transaction identifier (UTID), instead of a separate authorization system doing it. A transaction administrator sends a UTID to the customers computer, and the customer validates the transaction by comparing the UTID provided by the transaction administrator with a list of UTIDs stored on the customer's computer. ("[T]he transaction administrator 60 . . . transmits the data to the originator 50 and requests that the originator validate the transaction request containing the UTID at step 90." (5:8-11) The originator 50 validates the transaction by comparing at step 95 the

UTID with a list 100 generated by the processor 70.” (5:14-16) The processor 70 is the user/customer’s own personal computer. (4:49-50, 58-63).

Basically, Talati’s transaction administrator knows the customer’s email or telephone number and calls the customer to say “Hey, did you make this transaction?” The customer replies “yeah, that’s me” or “no, that’s not me.” Of course this only works from the customer’s home (for phone number) or when the customer is logged into a particular account (for email) because the transaction administrator has to make a separate call. This is very different from the present application which has the authorization system, and not the customer, validate the transaction. In this way, the customer can be anywhere, as long as she knows her authentication phrase.

Claim 21

Furthermore, as for dependent claim 21, while Talati’s UTID is only used for one single “unique” transaction, the single authentication phrase of claim 21 is used for multiple transactions.

Claim 28

Claim 28 stands rejected under 103 in light of Talati and Lineham. This rejection is respectfully traversed.

Claim 28 requires that the authorization form be provided “to a node indicated by the first user information.” The first user information is received “at a central authorization facility” by “a first merchant.” This is the opposite to Talati, which receives the node indication information separately and independently from the merchant. In fact, it is this very feature (that the authorization knows where the customer is supposed to be, such as an email address or telephone number, and contacts the customer in a separate communication) that allows Talati to obtain his desired security level.

Claims 12 and 26

Claims 12 and 26 are set apart for the use of a “logo” as a claim limitation. This rejection is respectfully traversed. To resolve the logo rejections and identify their


functional nature, these claims have been amended to use the term "information" instead of "logo."

Claim 6

Claim 6 stands rejected under 35 U.S.C. § 112. Claim 6 describes transforming the signature phrase "at the customer." In Fig. 1, the customer 14 is illustrated as being a computer. In the specification, the example of transformation discussed is a Hash function. To better clarify this claim element, claim 6 has been amended to identify that the transforming is done "by the customer."

An early formal notice of allowance of claims 6-9, 11-15, and 19-36 is requested. Permission is granted to use Deposit Account No. 08-1394 if required.

Respectfully submitted,



David M. O'Dell
Registration No. 42,044

Date: August 28, 2002

HAYNES AND BOONE, LLP
Attorney Docket No. 26796.2
901 Main Street, Suite 3100
Dallas, Texas 75202-3789
Telephone: 972/739-8635
Facsimile: 972/680-7551



27683

PATENT TRADEMARK OFFICE

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Box AF, Commissioner For Patents, Box AF, Washington, D.C. 20231

On: August 28, 2002
By: Marsha S. Green
Marsha S. Green

R-29162.1



Marked-up Version of Claim Amendments

6. (Amended) The method of claim 13 wherein the authorization form includes a transformation system to transform the signature phrase [at] by the customer, and wherein the interface receives the second account number and the second signature phrase in a transformed format.

12. (Amended) The method of claim 13 wherein the authorization form includes [a logo] information identifying the merchant.

26. (Amended) The method of claim 22 wherein the authorization form includes [a logo] information associated with the authorization system.